

ABSTRACT

KEY DERIVATION METHOD, APPARATUS, AND SYSTEM

Embodiments of this application disclose a key derivation method, an apparatus, and a system. The method includes: User equipment UE receives an authentication success message from a mobility management function network element, generates a master session key MSK and an extended master session key EMSK based on the authentication success message; and determines whether an authentication device is located outside a 3rd generation partnership project 3GPP network, to determine whether to obtain Kausf based on the EMSK or the MSK. Therefore, the UE can be compatible with a key derivation manner used when the authentication device is located outside the 3GPP network and a key derivation manner used when the authentication device is located inside the 3GPP network.

Figure 2